UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/457,732	12/10/1999	ANDREA CALIFANO	YO999-137	8003

21254 7590 01/17/2008

MCGINN INTELLECTUAL PROPERTY LAW GROUP, PLLC
8321 OLD COURTHOUSE ROAD
SUITE 200
VIENNA, VA 22182-3817

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
01/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

33UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/457,732
Filing Date: December 10, 1999
Appellant(s): CALIFANO ET AL.

Scott Tulino (Reg. No. 48,317
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 26 November 2007 appealing from the Office action mailed 22 June 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Menezes, Alfred et al. Handbook of Applied Cryptography. 1997. CRC Press LLC. p. 321-375.

6,446,210	BORZA	09-2002
6,487,662	KHARON et al.	11-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 14-16, 31, and 32 are rejected under 35 U.S.C. 101 because the disclosed invention is inoperative and therefore lacks utility. Claims 1, 14-16, 31, and 32 all generally relate to comparing two separate, imperfect samples of biometric data using a hash function to provide authentication. The Examiner holds that such a method could not work, as evident by the **Handbook of Applied Cryptography** to Menezes et al., hereinafter Menezes. Chapter 9 of Menezes discloses the properties of hash functions. On page 331, Menezes proceeds to state one of the properties of one-way hash functions being near-collision resistance. Near-collision resistance is the property that states that "it should be hard to find any two inputs *x*, *x'* such that *h(x)* and *h(x')* differ in only a small number of bits." This is further supported by section **9.2.2 Basic properties and definitions**, on page 323 and 324.

Claims 31-36 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. On page 23 of the Specification, the Appellant describes a computer-readable medium (as discussed above drawn to the machine readable data storage medium) as being a transmission medium, such as digital and analog and communication links and wireless. The Office's current position is that claims involving signals encoded with functional descriptive material do not fall within any of the categories of patentable subject matter set forth in 35 U.S.C. § 101, and such claims are therefore ineligible for patent protection. *See* 1300 OG 142 (November 22, 2005) (in particular, see Annex IV(c)).

Claims 1, 5-8, 10-14, 16, 18-26, 28-32, and 34-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,446,210 to Borza, hereinafter Borza, in view of U.S. Patent No. 6,487,662 to Kharon et al., hereinafter Kharon.

As per claims 1, 13, 14, 16, 18, 20, 24-26, 28, 30-32, 34, and 36, Borza teaches a method of processing semiotic data, comprising:

receiving semiotic data including a data set P (Figures 3 [block 80], 5, 7a, 7b, 10, 11, 13, 14, 15; column 2, line 52 to column 3, line 23; column 8, lines 4-28);

selecting a function h, and for at least one of each said data set P to be collected, computing h(P) (Figure 5; column 7, line 45 to column 8, line 3);

destroying said data set P (column 2, lines 27-29); and

storing h(P) in a database (Figures 7a, 7b, 12; column 12, lines 39-53);

obtaining a sample of P' such that a comparison can be made (Figures 3 [block 80], 5, 7a, 7b, 10, 11, 13, 14, 15; column 2, line 52 to column 3, line 23; column 8, lines 4-28);

at least one of obtaining and computing h(P') (Figure 5; column 7, line 45 to column 8, line 3); and

to determine whether P' is close to a predetermined subject, comparing h(P) to all available h(P)s to determine whether P' substantially matches, but does not exactly match, one of said data set P (Figures 12, 13, 16, 17; column 8, lines 28-38, column 14, lines 21-59, column 16, lines 31-37, column 16, lines 53-58, i.e. "when the value is within predetermined limits for an acceptable value, identification is provided....when the value falls outside the predetermined limits identification is not provided");

wherein said data set P cannot be extracted from h(P) (column 8, lines 28-38);

wherein said semiotic data comprises biometric data (column 11, line 65 to column 12, line 18);

wherein said function h comprises a secure hash function (Figure 5; column 7, line 45 to column 8, line 3);

wherein the data set P is not determined perfectly by its reading (column 8, lines 28-38, column 14, lines 21-59, column 16, lines 61-37, column 16, lines 53-58)

wherein each reading gives a number Pi, wherein I is no less than 0, wherein P0 is for an initial reading, and a secret version of said initial reading is stored after further processing thereof (column 8, lines 28-48; column 11, lines 25-34; column 12, lines 25-61),

wherein reading P0 is different from Pi for i > 0, and the secret version of P0 is different from the secret version of Pi, such that no identification is possibly by a direct comparison of the encrypted data (Figures 7b, 9-11, 14, 18; column 13, lines 1-21, column 14, line 60 to column 15, line 63, column 16, line 58 to column 17, line 14),

each time a Pi, with i > 0, is read, computing all possible predetermined size variations of Pi which correspond to an acceptable predetermined imprecision of the reading (column 11, lines 25-34; column 12, lines 25-61); and

encrypting all such modified data, and comparing said encrypted modified data to data stored in said database (column 8, lines 28-48; column 12, lines 25-61),

wherein for a plurality of users of the same biometric information, said biometric information is encrypted differently for each user (column 4, lines 46-58; column 5, lines 42-55),

wherein at least one of said data set P and P` comprises a personal data set (column 12, lines 25-34).

Borza does not teach extracting sub-collections Sj from the collection of data in data set P; and encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

Kharon teaches further comprising:

extracting sub-collections Sj from the collection of data in data set P (Figure 6 [block 340]; column 13, lines 43-67); and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability (Figure 6 [block 347]; column 13, lines 43-67);

comparing encrypted versions of the sub-collections Sj with those data stored in said database (Figure 6 [blocks 345, 347]; column 13, lines 43-67; column 14, lines 28-39; column 15, lines 42-55),

wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred (Figure 6 [blocks 345, 347]; column 13, lines 43-67; column 14, lines 28-39; column 15, lines 42-55). It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification.

As per claim 5, Borza teaches a method of processing semiotic data, comprising:

receiving semiotic data including a data set P (Figures 3 [block 80], 5, 7a, 7b, 10, 11, 13, 14, 15; column 2, line 52 to column 3, line 23; column 8, lines 4-28);

selecting a function h, and for at least one of each said data set P to be collected, computing h(P) (Figure 5; column 7, line 45 to column 8, line 3);

destroying said data set P (column 2, lines 27-29); and

storing h(P) in a database (Figures 7a, 7b, 12; column 12, lines 39-53); and

wherein said data set P cannot be extracted from h(P) (column 8, lines 28-38);

the method further comprising:

selecting a private key/public key (K, k) once for all cases (column 4, lines 26-32); and

choosing said function h as the public encryption function corresponding to k (column 5, lines 28-54).

Borza does not teach destroying said private key K and sending said private key K to a trusted party. It would have been obvious to one having ordinary skill in the art at the time the invention was made to destroy the private key K and send it the private key K to a trusted third party, since it is known in the art that the private key is needed to decrypt any message encrypted with public key k, therefore the fewer entities that have access to private key K equals the fewer number of people that can access messages encrypted with public key k.

Regarding claim 6, Borza teaches wherein said data set P cannot be extracted from h(P), except by the trusted party (column 8, lines 28-38).

Regarding claim 7, Borza teaches to determine whether some P' is a predetermined subject, comparing said h(P) to all available h(P)s (column 12, lines 48-61); and

determining whether there is a match (column 12, lines 48-61).

Regarding claim 8, Borza does not teach wherein the trusted party comprises a panel of members, and wherein a secret is shared among the members so that only at least a predetermined number of panel members can reconstitute the secret in its entirety by putting together their share of the secret. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the trusted party to comprise of a panel of members, and share a secret is amongst the members so that only at least a predetermined number of panel members can reconstitute the secret in its entirety by putting together their share of the secret, since it has been held that mere duplication of essential elements (e.g. trusted third party) involves only routine skill in the art. *St. Regis Paper Co. v. Bemis Co.,* 193 USPQ 8. See also MPEP § 2144.04.

Regarding claim 10, Borza does not teach extracting sub-collections Sj from the collection of data in data set P; and encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

Kharon teaches extracting sub-collections Sj from the collection of data in data set P (Figure 6 [block 340]; column 13, lines 43-67); and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability (Figure 6 [block 347]; column 13, lines 43-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification.

With regards to claims 11 and 21, Borza does not teach comparing encrypted versions of the sub-collections Sj with those data stored in said database, wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred.

Kharon teaches comparing encrypted versions of the sub-collections Sj with those data stored in said database (Figure 6 [blocks 345, 347]; column 13, lines 43-67; column 14, lines 28-39; column 15, lines 42-55),

wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred (Figure 6 [blocks 345, 347]; column 13, lines 43-67; column 14, lines 28-39; column 15, lines 42-55). It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification.

Concerning claims 12 and 23, Borza teaches each time a Pi, with i > 0, is read, computing all possible predetermined size variations of Pi which correspond to an acceptable predetermined imprecision of the reading (column 11, lines 25-34; column 12, lines 25-61); and

encrypting all such modified data, and comparing said encrypted modified data to data stored in said database (column 8, lines 28-48; column 12, lines 25-61).

As per claims 19, 29, and 35, Borza teaches a method of extracting components of biometric data which are stable under measurement errors, comprising:

acquiring unencrypted biometric data including at least one data set P (Figure 3 [block 80]; column 8, lines 4-28);

encrypting each said at least one data set acquired to form at least one encrypted data set (Figure 3 [block 73]; column 5, lines 42-54; column 8, lines 28-38);

destroying the unencrypted data set P (column 2, lines 27-29); and

storing each said at least one encrypted data set in a database (Figures 7a, 7b, 12; column 8, lines 28-48; column 12, lines 39-53),

wherein unencrypted biometric data is not available nor retrievable from said data stored in said database (column 8, lines 28-38).

Borza does not teach extracting sub-collections Sj from the collection of data in data set P; and encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

Kharon teaches further comprising:

extracting sub-collections Sj from the collection of data in data set P (Figure 6 [block 340]; column 13, lines 43-67); and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability (Figure 6 [block 347]; column 13, lines 43-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification.

Regarding claim 22, Borza teaches wherein the data set P is not determined perfectly by its reading, such that each reading gives a number Pi,

wherein i is no less than 0 (column 11, line 65 to column 12, line 34),

wherein P0 is for an initial reading, and a secret version of said initial reading is stored after further processing thereof (column 11, line 65 to column 12, line 34),

wherein reading P0 is different from Pi for i > 0, and the secret version of P0 is different from the secret version of Pi, such that no identification is possible by a direct comparison of the encrypted data (column 11, line 65 to column 12, line 34).

Claims 9, 15, 17, 27, and 33 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,446,210 to Borza, hereinafter Borza.

As per claim 9, Borza teaches a method of processing semiotic data, comprising:

receiving semiotic data including a data set P (Figures 3 [block 80], 5, 7a, 7b, 10, 11, 13, 14, 15; column 2, line 52 to column 3, line 23; column 8, lines 4-28);

selecting a function h, and for at least one of each said data set P to be collected, computing h(P) (Figure 5; column 7, line 45 to column 8, line 3);

destroying said data set P (column 2, lines 27-29); and

storing h(P) in a database (Figures 7a, 7b, 12; column 12, lines 39-53); and

wherein said data set P cannot be extracted from h(P) (column 8, lines 28-38);

wherein the data set P is not determined perfectly by its reading (column 11, lines 25-34), wherein each reading gives a number Pi, wherein i is no less than 0, wherein P0 is for an initial reading, and a secret version of said initial reading is stored after further processing thereof (column 11, line 65 to column 12, line 34),

wherein reading P0 is different from Pi for i > 0, and the secret version of P0 is different from the secret version of Pi, such that no identification is possible by a direct comparison of the encrypted data (column 11, line 65 to column 12, line 34).

As per claims 15, 17, 27, and 33, Borza teaches a method of processing biometric data, comprising:

acquiring unencrypted biometric data including at least one data set P (Figure 3 [block 80]; column 8, lines 4-28);

encrypting, with one of a secure hash function and an identity function, each said at least one data set acquired (Figure 3 [block 73]; column 5, lines 42-54; column 8, lines 28-38);

destroying the unencrypted data set P (column 2, lines 27-29);

storing each of the at least one encrypted data set in a database (Figures 7a, 7b, 12; column 8, lines 28-48; column 12, lines 39-53),

wherein unencrypted biometric data is not available nor retrievable from said data stored in said database (column 8, lines 28-38),

to determine whether a data set P` is a predetermined subject, comparing an encrypted data set of P` to the at least one encrypted data set stored in the database to determine whether there is a match (Figure 12; column 8, lines 28-38).

(10) Response to Argument

Response to Arguments concerning 35 U.S.C. 101 rejection – Inoperable

In response to the Appellant's position that the Examiner did not respond to or answer the substance of the Appellant's traversal, the Examiner disagrees. In response to a proper 35 U.S.C. 101 rejection, the burden shifts to the appellant to rebut the prima facie showing. The Appellant may rebut this rejection using any combination of the following: amendments to the claims, arguments or reasoning, or new evidence submitted in an affidavit or declaration under 37 CFR 1.132, or in a printed publication. In response to the requirement, the Appellant did not amend the claims, submit an affidavit or declaration, or a printed publication to rebut the Examiner's rejection. Instead the Appellant chose to argue by referring back to the specification of the instant application and arguing that the hashes produced are close. The Appellant is reminded that the features upon which appellant relies, such as the methods disclosed in the specification, are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The Examiner has considered the specification, claims, and prior art before making the rejection and believes the asserted utility would be incredible to a person of ordinary skill in the art. See *In re Rinehart*, 531 F.2d 1048, 1052, 189 USPQ 143, 147 (CCPA 1976).

The Appellant failed to properly address the Examiner's *prima facie* showing of the inoperability of the instant invention and the Examiner responded in the only method available at the time, and as such the rejection should be maintained.

In response to the Appellant's arguments that the Examiner is not considering the Appellant's actual argument or the actual disclosure of the invention, the Examiner disagrees. The Appellant agrees with the Examiner's position that a simple hash function would not work on page 26 of the Appeal Brief filed 07 September 2006. The Appellant refers to methods for circumventing the problems of comparing encrypted or hashed data samples but is reminded that the features upon which appellant relies are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). In other words, while the specification may disclose methods of performing the biometric authentication using a hash function, the claim language is not as specific as the Appellant's specification in disclosing how the hash function is applied to the biometric data.

Furthermore, the Examiner would like to point out that the Appellant fails to define/redefine the term hash function to coincide with a particular method disclosed in the specification. Where appellant acts as his or her own lexicographer to specifically define a term of a claim contrary to its ordinary meaning, the written description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the appellant intended to so redefine that claim term. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The Appellant has not elaborated in the claim language that the hash function is one of the disclosed methods on pages 17-20 of the specification. The Appellant fails to meet the requirements of redefining a term as set forth in the MPEP § 2106. In order to define/redefine a term, the Appellant must do so "with reasonable clarity, deliberateness, and precision" and must "set out his uncommon definition in some manner within the patent disclosure' so as to give one of ordinary skill in the art notice of the change" in meaning.

The Examiner has considered the claim language as a whole and in light of the specification, and has refrained from reading limitations from the specification into the claim language, especially giving the "hash function" its broadest reasonable interpretation. The Examiner does not disagree with the Appellant that the disclosure of the invention is operable, but the claim language as broadly interpreted by the Examiner provides for an inoperable invention and the rejection should be maintained.

Finally, in response to the Appellant's arguments that the claimed invention does not use a hash function by itself. The Examiner notes that the Appellant has failed to define h in the claims as anything more than a secure hash function. The Examiner believes that further defining h as more than just a hash function would help to distinguish the instant invention over the prior art, as well as obviate the rejection under 35 U.S.C. 101, as was noted in the Advisory Action of 29 August 2007. It is noted that the features upon which appellant relies, namely that the function h comprises more than just a secure hash function, are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Response to Arguments concerning 35 U.S.C. 101 rejection – Non-statutory

The Examiner disagrees with the Appellant's allegations that claims 31-36 are directed toward statutory subject matter. As noted in the previous Office Action, the Appellant has failed to define what a computer-readable medium is in the specification. The closest definition the Examiner could find was that of a machine readable data storage medium on page 23, lines 10-16 of the specification, which states:

> the instructions may be stored on a variety of machine-readable data storage media, such as DASD storage (e.g., a conventional “hard drive” or a RAID array), magnetic tap, electronic read-only memory (e.g., ROM, EPROM, or EEPROM), an optical storage device (e.g. CD-ROM, WORM, DVD, digital optical tap, etc.), paper "punch" cards, or other suitable signal bearing media including transmission media such as digital and analog and communication links and wireless (emphasis added)

As noted in the Office Action of 22 June 2007, the Office's current position is that claims involving signals encoded with functional descriptive material do not fall within any of the categories of patentable subject matter set forth in 35 U.S.C. § 101, and such claims are therefore ineligible for patent protection. See 1300 OG 142 (November 22, 2005) (in particular, see Annex IV(c)). Furthermore, the Appellant's claimed computer-readable medium could reasonable comprises ethernet or coaxial cables, thereby rendering the claimed subject matter nonstatutory since it would comprise signal or carrier waves. Further defining the differences between a "computer readable medium" or a "computer storage medium" and a "transmission medium" in the specification would assist in resolving the statutory matters regarding claims 31-36.

Response to Arguments concerning 35 U.S.C. 103 prior art rejection

In response to appellant's argument that the claimed invention provides a method and system for processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, without significantly altering the accuracy and sensitivity of the identification process, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim. See MPEE § 2105; see *In re Schreiber*, 128 F.3d 1473, 17477, 44 USPQ2d 1429, 1431 (Fed. Cir. 1997).

In response to appellant's argument that the references fail to show certain features of appellant's invention, it is noted that the features, such as how the comparison between the two data sets are compared, upon which appellant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The Appellant does not claim the structure that does the comparing between the two encrypted samples, but instead claims the method steps which the Examiner has shown to be taught by *Borza*.

In response to the Appellant's arguments that *Borza* does not determine whether h(P) is close to h(P`), the Examiner disagrees. *Borza* discloses at column 16, lines 19-38 discloses techniques for determining the identification of someone by acquiring a biometric sample and comparing it to the stored templates. If the sample acquired for authentication is within predetermined range of the template, identification is provided for, if it is outside that predetermined range, then the user is not authenticated. *Borza* teaches comparing encrypted samples to encrypted templates in column 8, lines 28-38. The Appellant is reminded of MPEP 2123, which states that patents are relevant as prior art for all they contain.

Borza discloses determining whether h(P) is close to h(P`), without having to be identical matches, when comparing encrypted samples to encrypted templates, and the rejection should be maintained.

In response to the Appellant's argument that *Kharon* does not disclose extracting multiple subsets of data. In column 14, lines 40-53 *Kharon* discloses the kth minutia and groupings of minutia. *Kharon* also states at column 13, lines 63-67 that the data set is defined so that N represents the total number of minutia for the fingerprint.

Kharon discloses extracting multiple subsets from the data in disclosing multiple instances of the minutia, and the rejection should be upheld.

In response to the Appellant's argument that *Kharon* does not teaches comparing encrypted versions of the sub-collection with those stored in the database, the Examiner disagrees. As shown above, *Borza* provides a showing of comparing two encrypted data sets for authentication purposes. *Kharon* teaches at column 14, lines 1-9 of comparing the minutia data sets to that of a database for authenticating the fingerprint.

Therefore, the combination of references discloses comparing encrypted subsets of data against a database for verification and the rejection should be maintained.

In response to appellant's argument that the claimed invention using a smaller subset of data for verification would be less desirable since it is easy to forge the data and does not solve the problem of being able to compare two encrypted data sets, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

Appellant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

In response to appellant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

In response to appellant's argument that the references fail to show certain features of appellant's invention, it is noted that the features upon which appellant relies, such as extracting subsets of data and comparing encrypted subsets of data, are not recited in all of the rejected independent claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/CLF/
Christian LaForgia
Patent Examiner
Art Unit 2131

GILBERTO BARRON Jr
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:
Gilberto Barron, Jr.
Supervisory Patent Examiner
At Unit 2131

Matthew Smithers

/Matthew Smithers/
Primary Examiner
Art Unit 2137